

REMARKS

Applicant appreciates the Examiner's thorough examination of the subject application and request reexamination and reconsideration of the subject application in view of the preceding amendments and following remarks. Applicant has carefully reviewed and considered the Office Action mailed on December 21, 2007, and the references cited therewith. Reconsideration and allowance of the subject application, as amended, are respectfully requested.

Claims 1-6, 8-13, 15 and 16 are pending in this application.

35 USC §101 Rejection of the Claims

Claims 1-6, 8-13 and 15 stand rejected under 35 USC § 101 as being directed towards non-statutory subject matter. Applicant respectfully traverses this rejection.

The Examiner states "the claimed system must include hardware necessary to realize any of the functionality of the claimed modules and produce a useful, concrete and tangible result." *Official Action*, page 2. Applicant's independent claim 1 is provided below for the Examiner's convenience.

1. (Previously Presented): An integrated firewall/VPN system, comprising:

at least one wide area network (WAN);

at least one local area network (LAN); and

an integrated firewall/VPN chipset configured to send and receive data packets between said WAN and said LAN, said chipset comprising:

a firewall comprising a first layer including a header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking;

a VPN configured to provide security functions for data between said LAN and said WAN, wherein said security functions are selected from the group consisting of encryption, decryption, encapsulation, and decapsulation of said data packets, said VPN including a VPN packet buffer configured to receive at least one of said data packets and to forward said at least one data packet to an inbound VPN processor configured to decrypt and decapsulate said at least one data packet, said VPN further including an inbound security database having a database of tunnels configured to provide said inbound VPN processor with tunnel information used to decrypt and decapsulate said at least one data packet, said VPN further including protocol instructions having microcodes configured to instruct said VPN processor to decrypt and decapsulate said at least one data packet

according to a user-defined security procedure; and
an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text. (emphasis added).

Applicant respectfully submits that claim 1 includes hardware, i.e., an integrated firewall/VPN chipset. As shown above, the chipset includes a firewall, VPN and an interface configured to determine if the incoming data packets are plain text or cipher text. As such, Applicant respectfully submits that the rejection under 35 USC §101 be withdrawn. Independent claims 9 (an IC comprising a router core) and 16 (receiving data packets at an interface, a hardware engine configured to provide pre-analysis processing, etc.) include similar limitations and are believed to be directed towards statutory subject matter as well.

35 USC §103 Rejection of the Claims

Claims 1-3, 9 and 10 stand rejected under 35 USC § 103(a) as being unpatentable over Vairavan (US Pub. No. 2002/0083344) in view of Hui et al (US Pub. No. 2004/0010712) in view of Canon et al (US Patent No. 2002/0108059) in view of Foschiano et al (US Pub. No. 2004/0022253) and in view of Yang et al (US Patent No. 7,003,118). Applicant respectfully traverses this rejection.

As an initial matter, Applicant respectfully submits that the Examiner has not shown where the cited references teach each and every limitation of Applicant's claims as a whole. While it is within the Examiner's right to combine references in a 35 USC 103 rejection, it is incumbent upon the Examiner to show how a person of ordinary skill in the art would know how to combine these references to create Applicant's invention. Applicant respectfully submits that the Examiner has conveniently selected a number of individual components of each limitation from a variety of different references in effect creating a 'patchwork quilt' to suit his rejection. In order to effectively respond to the Examiner's rejection, Applicant respectfully requests that the Examiner show precisely where each limitation as a whole is taught in the prior art.

Applicant's claim 1 is directed towards an integrated firewall/VPN chipset. That is, the firewall and VPN are both located in the chipset. The firewall includes "a first layer including a

header match packet filtering engine configured to provide pattern matching in selected headers of data, a second layer including a contents match packet filtering engine configured to analyze the scope of at least one data packet, a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU) and a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up-table and to forward the setup progress to said CPU for tracking.”

In the Official Action, the Examiner appears to rely upon Hui as teaching “a third layer including at least one application proxy configured to provide additional pattern matching.” *Official Action*, page 4. However, Applicant respectfully submits that Hui fails to teach the limitation as a whole, i.e., “a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU).” Specifically, Applicant is unable to find reference to a hardware engine configured to provide pre-analysis processing to reduce the workload of a central CPU in Hui.

The Examiner then appears to rely upon Foschiano as teaching “a hardware engine to provide pre-analysis processing to reduce the workload of a central processing unit (CPU).” *Official Action*, page 5. Again, Applicant respectfully submits that the Examiner has failed to show precisely where this limitation as a whole is taught in the prior art. Neither Hui nor Foschiano appear to teach “a third layer including at least one application proxy configured to provide additional pattern matching using a hardware engine configured to provide pre-analysis processing to reduce the workload of a central processing unit (CPU).” Moreover, it is unclear to Applicant why a person of ordinary skill in the art would combine these two references in the manner described by the Examiner.

On page 4 of the Official Action, the Examiner seems to suggest that Canion teaches “a fourth layer including a session match engine configured to store a TCP/UDP connection setup in a look-up table and to forward the setup progress to said CPU for tracking.” *Official Action*, page 4. Applicant respectfully disagrees with this determination. Applicant is unable to find any

reference to a look-up table in Canon. Further, Applicant is also unable to find any reference in Canon to forwarding “the setup process to said CPU for tracking.”

On page 5 of the Official Action, the Examiner seems to suggest that Vairavan teaches the interface of Applicant’s claim 1. Applicant respectfully disagrees. Specifically, it is Applicant’s belief that Vairavan does not teach “an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.” Paragraph [0022] of the subject application discusses the benefits of the analysis of preselected data. This section has been provided below for the Examiner’s convenience.

[0022] In the present invention, the firewall 220 is adapted with appropriate hardware and software to analyze the preselected data instead of having to operate on the entire data packet. This can increase the overall speed and efficiency of the firewall. Those skilled in the art will recognize that larger portions of preselected data will increase security, but may tend to slow down the firewall processing. Therefore, the present invention permits users to “tune” the firewall settings to meet desired security and/or speed requirements. *Subject application, para. [0022]. Emphasis added.*

Thus, as discussed above, the firewall may analyze preselected data to “increase the overall speed and efficiency of the firewall.” Applicant is unable to find any discussion of this in Vairavan. Specifically, Applicant is unable to find reference to “an interface configured to determine if said data packets are plain text or cipher text, said interface further configured to forward a preselected number of bytes to said firewall if said data packets are plain text, said interface further configured to forward said data packets to said VPN if said data packets are cipher text.” The Examiner appears to rely upon paragraph [0132] of Vairavan as teaching this limitation. However, it is Applicant’s understanding that Vairavan merely teaches a firewall filter configured to pass or discard an entire packet. Applicant’s are unable to find reference to “an interface configured to forward a preselected number of bytes to said firewall if said data packets are plain text” as required by Applicant’s claim 1.

Therefore, Applicant respectfully submits that independent claim 1 is in condition for allowance. Independent claims 9 and 16 include similar limitations and are believed to be in

AMENDMENT

Serial Number: 10/658,561

Filing Date: September 8, 2003

Title: VPN AND FIREWALL INTEGRATED SYSTEM

Page 11

Docket: O2M02.20

condition for allowance as well. Since the remaining dependent claims depend either directly or indirectly from Applicant's independent claims, Applicant respectfully submits that these claims are in condition for allowance as well.

Having dealt with all the objections raised by the Examiner, it is respectfully submitted that the present application, as amended, is in condition for allowance. Thus, early allowance is earnestly solicited.

If the Examiner desires personal contact for further disposition of this case, the Examiner is invited to call the undersigned Attorney at 603.668.6560.

In the event there are any fees due, please charge them to our Deposit Account No. 50-2121.

Respectfully submitted,

By: /Edmund P. Pfleger/
Edmund P. Pfleger
Reg. No. 41,252